

Utilisation partielle du CRC pour la correction d'erreurs des signaux AIS reçus par satellite

Raoul PRÉVOST¹, Martial COULON², David BONACCI¹, Julia LE MAITRE³,
Jean-Pierre MILLERIOUX³ et Jean-Yves TOURNERET²

¹TéSA, 7 boulevard de la Gare, 31500 Toulouse, France

²Université de Toulouse, INP-ENSEEIH/IRIT, 2 rue Charles Camichel, BP 7122, 31071 Toulouse cedex 7, France

³CNES, 18 Avenue Edouard Belin, 31400 Toulouse, France

{raoul.prevast, david.bonacci}@tesa.prd.fr,
{martial.coulon, jean-yves.tourneret}@enseeiht.fr,
{julia.lemaitre, jean-pierre.millerioux}@cnes.fr

Résumé – Cet article s'intéresse à la démodulation des signaux du système d'identification automatique (AIS) reçus par satellite. Plus précisément, il présente un algorithme de correction d'erreurs dont la complexité calculatoire est réduite par rapport à une précédente approche. Cette dernière utilisait le contrôle de redondance cyclique (CRC) d'un message comme une source de redondance afin d'en corriger les erreurs de transmission. Dans cet article, le CRC est également employé comme moyen de correction, mais en n'en utilisant qu'une partie seulement. Le reste peut être exploité pour la détection des erreurs. Cette nouvelle approche permet d'adapter les performances de décodage au niveau de bruit et de réduire la complexité calculatoire. Les résultats de simulation obtenus avec et sans optimisation de la complexité sont présentés et comparés dans le contexte du système AIS.

Abstract – This paper deals with the demodulation of automatic identification system (AIS) signals received by a satellite. More precisely, an error correction algorithm is presented, whose computational complexity is reduced with respect to that of a previously considered approach. This latter approach makes use of the cyclic redundancy check (CRC) of a message as redundancy, in order to correct transmission errors. In this paper, the CRC is also considered as a correction tool, but only a part of it is used for that purpose; the remaining part is only used as an error detection means. This novel approach allows the decoding performance to be adapted to the noise power, and provides a reduction of the computational complexity. Simulation results obtained with and without complexity optimization are presented and compared in the context of the AIS system.

1 Introduction

L'objectif de cet article est de présenter un algorithme de démodulation optimisé pour les signaux du système d'identification automatique (AIS)[1] reçus par satellite. Le système AIS est un système de radiocommunication originellement créé afin d'éviter les collisions entre les navires. Celui-ci consiste en l'émission périodique de signaux de signalisation. Bien que ce système n'ait pas été conçu pour être reçu par satellite, il est possible d'en démoduler signaux enregistrés par satellite pour faire de la surveillance de trafic maritime globale. Quelques systèmes sont déjà opérationnels [2], et des études visant à augmenter les performances de détection sont en cours [3, 4, 5]. Dans un article précédent [6], nous avons proposé d'utiliser le contrôle de redondance cyclique (CRC) comme une source de redondance pour corriger les erreurs de transmission et ainsi augmenter le taux de détection des signaux AIS à faible rapport signal à bruit E_S/N_0 . Cet algorithme a ensuite évolué pour réduire sa sensibilité aux interférences [7] et pour suivre les fluctuations de phase [8]. La complexité de l'algorithme résultant est assez importante, et bien qu'il ne soit pas nécessaire que la détection soit réalisable en temps réel, il est intéressant de la réduire. C'est l'objectif de cet article.

La complexité de l'algorithme est essentiellement due au grand nombre d'états du treillis parcouru par l'algorithme de Viterbi pour corriger les erreurs de transmission en exploitant

le CRC. Le nombre d'états est égal à $4 \cdot 2^{N_{\text{CRC}}}$, où N_{CRC} est le nombre de bits du CRC. L'algorithme proposé dans cet article réduit le nombre de bits du CRC considérés pour la correction d'erreurs, réduisant ainsi le nombre d'états du treillis. En utilisant cet algorithme, il devient possible, par exemple, d'utiliser 8 bits du CRC pour corriger les erreurs, et de conserver les 8 bits restant pour la détection des erreurs résiduelles. Le nombre d'états du treillis est ainsi réduit d'un facteur $2^8 = 256$, conduisant à une accélération considérable des traitements. Dans cet article, un schéma adaptatif est proposé afin de minimiser la complexité tout en conservant des performances optimales. Celui-ci incrémente itérativement la taille de la partie du CRC utilisée pour la correction jusqu'à que plus aucune erreur ne soit détectée en utilisant la partie restante du CRC.

L'approche proposée dans [6] est basée sur l'application de l'algorithme de Viterbi sur un treillis particulier. Ce treillis, appelé treillis étendu, est composé des valeurs intermédiaires du calcul du CRC et du treillis de codage. De plus, les bits de bourrage sont pris en compte par l'inclusion de transitions spécifiques dans le treillis étendu. Des détails supplémentaires concernant cet algorithme sont disponibles dans [6, 9, 10]. La contribution principale de cet article est l'élaboration d'un treillis réduit ne considérant qu'une partie du CRC pour la construction des états étendus. La valeur du CRC complet calculée le long d'un chemin dans le treillis est alors stockée dans une nouvelle variable d'état et est utilisée pour calculer l'état

du CRC suivant lors d'une transition. Il reste possible d'appliquer la poursuite de la phase ainsi que l'amélioration de la correction proposées dans [8] et [11] au nouveau récepteur.

Cet article est organisé de la façon suivante : les caractéristiques de l'émetteur et le modèle du signal reçu sont présentés dans la section 2. La section 3 décrit l'algorithme de démodulation avec une attention particulière sur l'optimisation de la complexité proposée. Les résultats des simulations sont donnés dans la section 4. Enfin, les conclusions sont présentées section 5.

2 Caractéristiques du système AIS

Cet article ne considère que les signaux AIS reçus sans collision (la stratégie d'atténuation des interférences décrite dans [7] est applicable, mais n'est pas présentée ici par souci de concision). Les signaux AIS sont composés de 168 bits d'information, à partir desquels un CRC de 16 bits est calculé. Le CRC est concaténé aux bits d'information et la procédure d'insertion des bits de bourrage est appliquée à la séquence résultante. La séquence obtenue est ensuite transmise en utilisant le codage NRZI et la modulation GMSK. Les principales propriétés de l'émetteur sont rappelées ci-dessous.

2.1 Contrôle de redondance cyclique

Le CRC est défini comme la division (modulo 2) du polynôme obtenu à partir des données et d'un polynôme générateur standard. Le CRC peut également être calculé de manière itérative en l'initialisant à une valeur standard et en appliquant séquentiellement un opérateur pour chaque bit des données. Le schéma de l'opérateur itératif est présenté dans [6]. Cette possibilité permet d'effectuer le calcul du CRC en utilisant un treillis dont les états représentent les valeurs intermédiaires du calcul. Le CRC est généralement utilisé pour détecter les erreurs de transmission en comparant le CRC calculé à partir des données reçues et le CRC contenu dans la trame reçue. Un autre moyen de détecter les erreurs de transmission consiste à calculer le CRC global de la trame et de le comparer à zéro. En effet, aucune erreur de transmission n'est détectée lorsque ce CRC global est égal à zéro, c'est-à-dire,

$$\text{CRC}([\text{Données}, \text{CRC}(\text{Données})]) = 0. \quad (1)$$

Le CRC peut être utilisé comme un moyen de correction d'erreurs. En effet, le CRC est le résultat d'un calcul sur les données et contient donc une partie de l'information. Dans cet article, une partie du CRC est utilisé pour corriger les erreurs de transmission, tandis que l'autre partie est utilisée comme un outil de détection d'erreurs.

2.2 Codage et modulation

Des bits non informatifs 0 (bits de bourrage) sont insérés après chaque séquence de cinq bits 1 consécutifs. Cette procédure évite la présence de longues séquences de bits 1 qui pourraient entraîner une perte de synchronisation d'horloge. En outre, les bits 0 insérés évitent la présence de fanions de fin de trame à l'intérieur des données. Cette procédure est la raison principale de la grande complexité du correcteur proposé. En

effet, la présence de bits de bourrage dans les données rend les algorithmes classiques de correction d'erreurs à faible complexité inapplicables [6].

La séquence de bits obtenue après l'insertion des bits de bourrage est codée en NRZI (pour *non-return-to-zero inverted*) puis modulée en GMSK (pour *Gaussian minimum shift-keying*). Le module du signal à émettre obtenu après modulation est constant. Ce signal est défini ainsi

$$s(t) = e^{-j\theta(t; \mathbf{B})}$$

où la phase $\theta(t; \mathbf{B})$ contient les symboles d'information

$$\theta(t; \mathbf{B}) = 2\pi h \sum_{k=-\infty}^n b_k q(t - kT), \quad nT \leq t \leq (n+1)T. \quad (2)$$

Dans (2), T est la période symbole, $\mathbf{B} = \{b_k\}$ est la séquence de bits, h est l'indice de modulation et $q(t)$ est la forme d'onde GMSK [1]. Dans le système AIS, l'indice de modulation est fixé à $h = 0,5$.

2.3 Modèle du signal reçu

Dans cet article, on considère un canal à réponse fréquentielle uniforme dont le décalage en fréquence dû à l'effet Doppler et le délai sont connus du récepteur. Ces paramètres peuvent en effet être estimés par le récepteur en utilisant les symboles pilotes. En notant $s(t)$ le signal généré par le modulateur GMSK, le signal reçu peut être écrit de la façon suivante

$$r(t) = s(t) + n(t) \quad (3)$$

où $n(t)$ est un bruit blanc additif gaussien indépendant du signal transmis. L'objectif est de retrouver les données contenues dans le signal $s(t)$ à partir du signal $r(t)$.

3 Description du récepteur

3.1 Principe général

Le récepteur considéré dans cet article utilise une version modifiée de l'algorithme de Viterbi. Cet algorithme détermine la séquence de symboles de maximum de vraisemblance à partir du signal reçu (3). Le signal de K symboles reçu passe par un filtre adapté (FA) avant d'être échantillonné à un échantillon par symbole. On note r_k l'échantillon du signal reçu sur la k -ième période symbole. La séquence d'échantillons obtenue est ensuite traitée par l'algorithme de Viterbi dont la fonction de distance est le carré de la distance euclidienne

$$\sum_{k=1}^K |r_k - m_k|^2 \quad (4)$$

où m_k est l'échantillon du k -ième symbole estimé après filtrage adapté. En raison de la possible présence de bits de bourrage, l'algorithme de Viterbi est modifié de façon à intégrer des transmissions conditionnelles satisfaisant la contrainte suivante : le nombre de bits 1 consécutifs est limité à 5.

Pour que le CRC soit utilisé pour la correction d'erreurs, il est nécessaire de définir une contrainte spécifique dans le treillis. Dans [6] le CRC global était utilisé et contraint à satisfaire (1). Dans cet article seule une partie du CRC est utilisée.

Ainsi, seule cette partie du CRC global est contrainte à être égale à zéro. On note $\widetilde{\text{CRC}}$ cette partie du CRC utilisée pour la correction d'erreurs. Pour prendre en compte la contrainte $\widetilde{\text{CRC}} = 0$, un treillis étendu est développé, ses états (appelés états étendus) sont composés d'un état $\widetilde{\text{CRC}}$ et d'un état du codeur en treillis (CT). L'état étendu final dans le treillis étendu est choisi de façon à assurer que $\widetilde{\text{CRC}}$ est égal à zéro.

On note que la partie du CRC qui n'est pas contenue dans $\widetilde{\text{CRC}}$ peut être utilisée pour la détection des erreurs de transmission résiduelles dans le message décodé.

3.2 Construction du treillis étendu

Le CRC (et donc $\widetilde{\text{CRC}}$) peut être calculé itérativement, il est initialisé à une valeur standard et mis à jour pour chaque bit du message. Dans l'algorithme proposé dans [6], un treillis CRC est développé, ses états représentent les valeurs intermédiaires du calcul du CRC et les transmissions correspondent aux mises à jour du CRC par l'application de l'opérateur itératif. Deux transitions partent donc de chaque état CRC, une pour chaque valeur possible du bit appliqué à l'entrée de l'opérateur itératif. Dans cet article, un treillis $\widetilde{\text{CRC}}$ est développé avec des états représentant la première partie de la valeur du CRC. Par exemple, si chaque couple de lettres aa, bb, cc... représentent une valeur d'une partie du CRC, l'état $\widetilde{\text{CRC}}$ noté **aa** représente toutes les valeurs de CRC commençant par **aa**, c'est-à-dire, [**aaaa**], [**aabb**], [**aacc**]... Dans le treillis $\widetilde{\text{CRC}}$, un nombre limité de bits est utilisé pour connecter deux états $\widetilde{\text{CRC}}$. Si le CRC de valeur [**aabb**] est suivi par [**ccdd**] après mise à jour avec le bit 0 et par [**eeff**] après mise à jour avec le bit 1, alors des transmissions sont possibles, partant de l'état $\widetilde{\text{CRC}}$ **aa** et arrivant aux états $\widetilde{\text{CRC}}$ **cc** et **ee**, comme illustré par la figure 1.

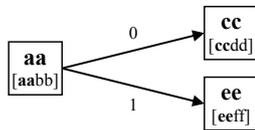


FIGURE 1 – Construction du treillis $\widetilde{\text{CRC}}$.

La valeur complète du CRC étant nécessaire pour en calculer la valeur suivante par application de l'opérateur itératif, une nouvelle variable d'état C est définie pour stocker cette valeur complète. À chaque étape de l'algorithme de Viterbi, la variable d'état C d'un état $\widetilde{\text{CRC}}$ donné est utilisée pour calculer les états $\widetilde{\text{CRC}}$ possibles suivants. La valeur complète du CRC mise à jour est alors stockée dans la variable d'état C des états $\widetilde{\text{CRC}}$ suivants.

Les états étendus sont définis par l'association d'un état $\widetilde{\text{CRC}}$ avec un état CT, les deux treillis associés évoluant en parallèle avec les mêmes bits. Cette association est illustrée dans (5), où l'entier k correspond au numéro du symbole reçu.

$$\begin{array}{ccc} \text{État } \widetilde{\text{CRC}} & \text{État CT} & \text{État étendu} \\ \begin{array}{c} \begin{array}{cc} k & k+1 \end{array} \\ A \xrightarrow{0} B \end{array} & \& \begin{array}{c} \begin{array}{cc} k & k+1 \end{array} \\ \alpha \xrightarrow{0} \beta \end{array} & \Rightarrow & \begin{array}{c} \begin{array}{cc} k & k+1 \end{array} \\ (A; \alpha) \xrightarrow{0} (B; \beta) \end{array} \\ \begin{array}{c} \begin{array}{cc} k & k+1 \end{array} \\ A \xrightarrow{1} C \end{array} & & \begin{array}{c} \begin{array}{cc} k & k+1 \end{array} \\ \alpha \xrightarrow{1} \gamma \end{array} & & \begin{array}{c} \begin{array}{cc} k & k+1 \end{array} \\ (A; \alpha) \xrightarrow{1} (C; \gamma) \end{array} \end{array} \quad (5)$$

Le nombre d'états du treillis étendu est égal au produit du nombre d'états du treillis $\widetilde{\text{CRC}}$ (c'est-à-dire, $2^{N_{\widetilde{\text{CRC}}}}$ avec $N_{\widetilde{\text{CRC}}}$ le nombre de bits de $\widetilde{\text{CRC}}$) et du treillis CT (c'est-à-dire, 4).

3.3 Bit de bourrage

Les bits de bourrage sont pris en compte par l'ajout de transitions spécifiques qui sont uniquement utilisées lorsqu'un bit de bourrage est reçu. La détection d'un tel bit est réalisée en utilisant le compteur P introduit dans [6]. Lorsque P atteint 5 le bit reçu est un bit de bourrage.

Les bits de bourrages étant insérés après le calcul du CRC à l'émission, le calcul du CRC ne doit pas non plus les prendre en compte à la réception.

4 Simulations

L'algorithme optimisé proposé dans cet article est comparé à l'algorithme original présenté dans [6]. Ils implémentent tous deux la stratégie de poursuite de la phase décrite dans [8]. Cette stratégie de poursuite de phase permet au récepteur d'être robuste au bruit de phase et aux indices de modulation h éloignés du standard. Dans ces simulations, les messages sont générés conformément à la recommandation AIS : ils sont composés de 168 bits d'information concaténés avec un CRC de 16 bits. Les bits de bourrage sont ensuite insérés. La trame est codée en NRZI, et modulée en GMSK avec un le paramètre $BT = 0,4$. Le polynôme générateur pour le CRC est $G(x) = x^{16} + x^{12} + x^5 + 1$. On considère un canal à bruit blanc gaussien additif (AWGN). Dans cet article, on suppose une synchronisation en temps et en fréquence parfaite. Les simulations sont effectuées sans introduire de bruit de phase : la mise en œuvre du suivi de phase est réalisée uniquement pour obtenir une estimation réaliste du temps de traitement.

L'algorithme proposé permet de sélectionner le nombre de bits du CRC $N_{\widetilde{\text{CRC}}}$ utilisés pour la correction d'erreurs entre 0 et 16. Ce nombre variable de bits est utile pour adapter le temps de traitement aux performances attendues. $N_{\widetilde{\text{CRC}}} = 0$ signifie qu'aucune correction n'est effectuée, $N_{\widetilde{\text{CRC}}} = 16$ donne les mêmes performances que l'algorithme de [6], tandis que $N_{\widetilde{\text{CRC}}} = 8$ permet d'obtenir des performances intermédiaires, avec un temps de calcul réduit par rapport au cas où $N_{\widetilde{\text{CRC}}} = 16$. Le tableau 1 présente les temps d'exécution mesurés sur un ordinateur de bureau, sur un cœur à 2,6 GHz, pour différentes valeurs de $N_{\widetilde{\text{CRC}}}$. La figure 2 montre les performances de démodulation en termes de taux d'erreur de paquet (TEP). On constate que le TEP diminue bien lorsque le nombre de bits de CRC utilisés pour la correction augmente.

De façon à optimiser les performances par rapport au temps d'exécution, nous proposons d'utiliser une structure itérative pour le récepteur. Celui-ci essaye de corriger le message en employant le minimum de bits de CRC, et augmente ce nombre de bits par étapes jusqu'à ne plus détecter d'erreurs de transmis-

TABLE 1 – Temps d'exécution

$N_{\widetilde{\text{CRC}}}$	Durée
0 bit	1,2 ms
8 bits	15,3 ms
12 bits	136,4 ms
16 bits	2074,0 ms

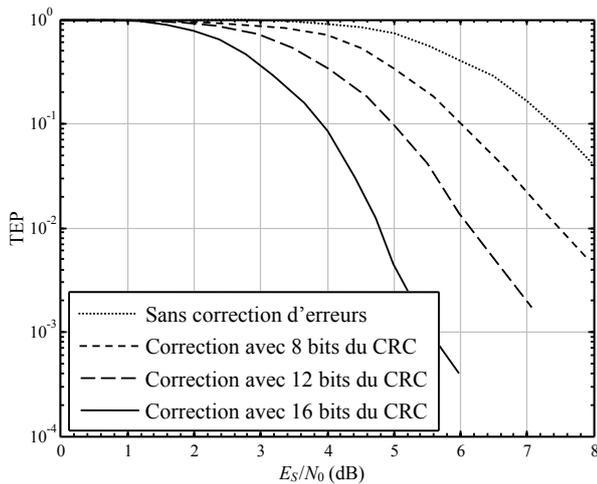


FIGURE 2 – TEP après correction. Comparaison des performances des correcteurs utilisant 0, 8, 12 et 16 bits du CRC.

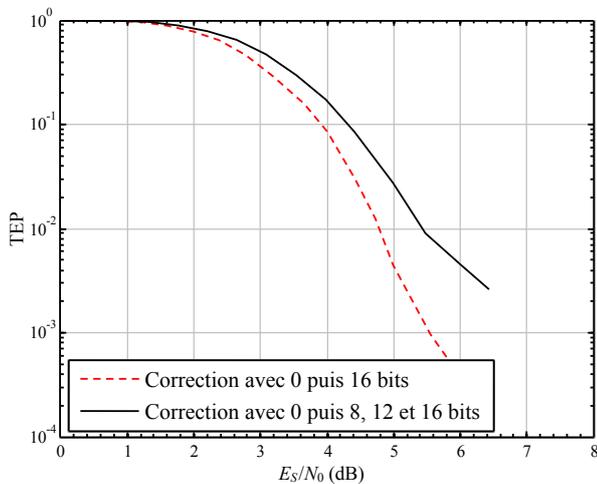


FIGURE 3 – TEP après correction. Le récepteur proposé est comparé avec celui présenté dans [6].

sion. On compare deux configurations :

- avec deux itérations sans nombre variable de bits de CRC pour la correction : $N_{\text{CRC}} = 0$ puis 16,
- en utilisant le correcteur proposé qui peut considérer un nombre variable de bits du CRC pour la correction. On définit 4 itérations, avec 0, 8, 12 puis 16 bits du CRC pour la correction.

Les courbes de TEP présentées dans la figure 3 montrent que les performances de la stratégie proposée sont très proches de celles de l’algorithme original (les différences sont dues à la probabilité de non-détection des erreurs de chaque itération), alors que les temps de calcul présentés dans la figure 4 sont grandement réduits. La stratégie proposée est en moyenne 10 fois plus rapide que celle n’employant pas le correcteur proposé lorsque le rapport signal à bruit se situe entre 5 et 10 dB.

5 Conclusion

Cet article a présenté une évolution d’un algorithme de démodulation des signaux AIS reçus par un satellite. Cet algorithme utilise un treillis étendu de façon à profiter du CRC inclus dans les messages pour corriger les erreurs de transmis-

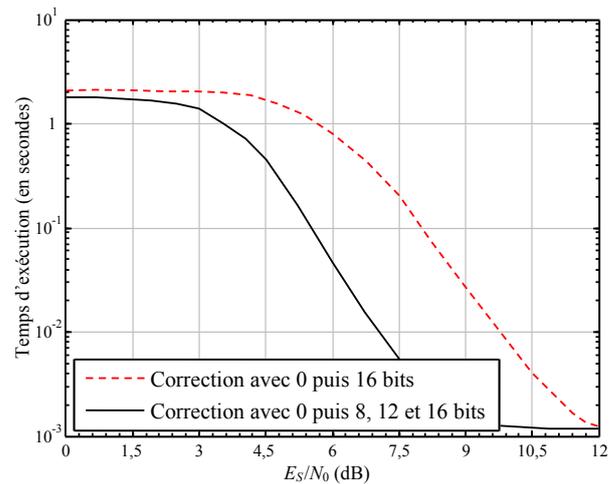


FIGURE 4 – Temps moyen de décodage. Le récepteur proposé est comparé avec celui présenté dans [6].

sion. Le principal avantage de l’évolution proposée est l’optimisation de la complexité calculatoire en n’exploitant qu’une partie du CRC pour la correction d’erreurs. Cet article a également présenté une procédure itérative permettant de conserver les très bonnes performances du correcteur original tout en divisant son temps d’exécution moyen par un facteur 10. Les prochains développements se concentreront sur l’optimisation de la procédure itérative afin de sélectionner la valeur optimale de N_{CRC} de chaque itération.

Références

- [1] RECOMMENDATION ITU-R M.1371, « Technical characteristics for a universal automatic identification system using time division multiple access in the VHF maritime mobile band », ITU, 2001.
- [2] « exactEarth », <http://www.exactearth.com>, 2010.
- [3] M. ZHOU, A. van der VEEN et R. van LEUKEN, « Multi-user LEO-satellite receiver for robust space detection of AIS messages », in *Proc. IEEE Int. Conf. Acoust., Speech, and Signal Processing*, vol. 37, (Kyoto, Japan), p. 2529–2532, Mar. 2012.
- [4] N. BOUNY, J. LE MAITRE et J.-P. MILLERIOUX, « Results of measurement campaign for characterisation of AIS transmitters », in *Proc. Adv. Sat. Mul. Sys. Conf.*, vol. 12, (Baiona, Spain), p. 258–265, Sept. 2012.
- [5] M. PICARD, M. R. OULARBI, G. FLANDIN et S. HOUCHE, « An adaptive multi-user multi-antenna receiver for satellite-based AIS detection », in *Proc. Adv. Sat. Mul. Sys. Conf.*, vol. 12, (Baiona, Spain), p. 273–280, Sept. 2012.
- [6] R. PRÉVOST, M. COULON, D. BONACCI, J. LE MAITRE, J.-P. MILLERIOUX et J.-Y. TOURNERET, « CRC-assisted error correction in a trellis coded system with bit stuffing », in *Proc. IEEE Workshop on Stat. Signal Process.*, (Nice, France), p. 381–385, June 2011.
- [7] R. PRÉVOST, M. COULON, D. BONACCI, J. LE MAITRE, J.-P. MILLERIOUX et J.-Y. TOURNERET, « Interference mitigation and error correction method for AIS signals received by satellite », in *Proc. European Signal and Image Processing Conf.*, (Bucharest, Romania), p. 46–50, Aug. 2012.
- [8] R. PRÉVOST, M. COULON, D. BONACCI, J. LE MAITRE, J.-P. MILLERIOUX et J.-Y. TOURNERET, « Joint phase-recovery and demodulation-decoding of AIS signals received by satellite », in *Proc. IEEE Int. Conf. Acoust., Speech, and Signal Processing*, (Vancouver, Canada), p. 4913–4917, May 2013.
- [9] R. PRÉVOST, D. BONACCI, M. COULON, J. LE MAITRE, J.-P. MILLERIOUX et J.-Y. TOURNERET, « Multi-encodage error correction with extended trellis ». Patent.
- [10] R. PRÉVOST, D. BONACCI, M. COULON, J. LE MAITRE, J.-P. MILLERIOUX et J.-Y. TOURNERET, « A Viterbi algorithm with conditional transitions ». Patent.
- [11] R. PRÉVOST, M. COULON, D. BONACCI, J. LE MAITRE, J.-P. MILLERIOUX et J.-Y. TOURNERET, « Extended constrained Viterbi algorithm for AIS signals received by satellite », in *Proc. IEEE-AESS Conf. Telecom. Satellite*, (Rome, Italy), Oct. 2012.